APPLICATION FOR PATENT

INVENTORS:

RICHARD GLEE WOOD

JACK WHITE

TITLE:

PROCESS AND METHOD OF SCREENING AN INDIVIDUAL AT A POINT OF ENTRY TO A SECURE ENVIRONMENT TO ASCERTAIN A RISK FACTOR

CERTIFICATE OF EXPRESS MAIL

I hereby certify that this correspondence is being deposited by me with the United States Postal Service as "Express Mail Post Office to Addressee" Express Mail No. **ET 838 960 225 US** in an envelope addressed to MAIL STOP PATENT APPLICATION; Commissioner for Patents; PO Box 1450; Alexandria, VA, 22313-1450, on the following date: October 30, 2003

Christian Heausler

SPECIFICATION

FIELD

[0001] Embodiments pertain to methods for providing and tracking access of a registered or a non-registered individual to a secure environment at a point of entry.

[0002] Embodiments also pertain to forming a database, such as an authentication database on Risk Factors, for an individual and any associated items and wherein the database can be accessed by a smart card, biometrics reader, and/or other similar identification methods.

BACKGROUND

[0003] The present method is directed to a system and method for monitoring and regulating the entry of individuals to a secure area or secure environment, such as the transportation of people on an airplane or entry into a computer program. Each day, people move into and across the nation, who are likely to cause an act of terrorism. To provide protection against such an act, it is desirable that authorities be able to identify such individuals with certain levels of risk. In order to efficiently guard against potential terrorist attacks, authorities need to be able to detect any unusual or potentially dangerous activity and to notify the appropriate authorities if such activity were to occur.

[0004] Currently, the TSA has jurisdiction for most of the laws and regulations that relate to the transportation of people on airplanes in the United States. TSA does not, however, have any national mechanism to track the real-time movement of people, nor does it have any established mechanisms for coordinating information concerning the transportation of high risk people with law enforcement authorities.

[0005] Further exacerbating this problem is the lack of a single source of data or regulations regarding criminal individuals or individuals from dangerous countries with known cells of terrorism.

[0006] Data and regulations are dispersed between Immigration, police databases, Interpol, the FBI, CIA and state agencies. A need exists to gather this disparately sourced information into a single repository to establish a baseline for tracking these higher risk individuals.

[0007] While baggage checks have become common in the airline industry, there has been little or no screening of individuals prior to the boarding process. There have been little developments with access to police and other databases to make a company location secure. A quick method for screening has been needed that more correctly identifies potential terrorists.

SUMMARY

[0008] Embodiments include methods for providing access and tracking the access of a non-registered or registered individual at a secure point of entry to a secure environment. The methods entail an owner establishing a secure environment by an owner with the secure point of entry and an assigned environment Risk Factor. An individual, then, requests entry into the secured environment at the secure point of entry. An identifier signifying the individual is sent to an authentication database. The database notified the owner is the individual is registered or not.

[0009] If the individual is not registered, the owner than asks the individual questions in order to produce a profile based on the individual's answers. The owner then assigns the individual a Risk Factor based on the profile. The individual's Risk Factor is compared to the environment Risk Factor in order to ascertain whether the individual is authorized to enter the secured environment. The determination is then recorded in the authentication database.

[00010] If the individual is registered, the response from the authentication database also includes the Risk Factor assigned to the individual. The assigned individual Risk Factor is compared with the environment Risk Factor in order to determine whether the individual is granted access to the secured. The record of the determination is

sent to the authentication database.

[00011] The method also can entail the use of a smart card for entry into the authentication database.

[00012] The method also can entail the use of biometric identifiers for entry to the authentication database.

BRIEF DESCRIPTION OF THE DRAWINGS

[00013] The present method will be explained in greater detail with reference to the appended Figures, in which:

[00014] FIG 1 is a schematic of a method for providing access and tracking the access of an non-registered individual at a secure point of entry to a secure environment; and

[00015] FIG 2 is a schematic of method for providing access and tracking the access of a registered individual at a secure point of entry to a secure environment.

[00016] The present method is detailed below with reference to the listed Figures.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[00017] Before explaining the present method in detail, it is to be understood that the method is not limited to the particular embodiments herein and it can be practiced or carried out in various ways.

[00018] A need has existed for a risk assessment method and system that provides alarms or notification when certain levels of risk are detected for an individual attempting to enter or exit an environment that needs to be secured, namely a secure environment or a secure location. The risk factors are suggested by the definitions below, but additional criteria or elements that are common to immigration, border patrol or

police can be inserted or substituted for the items noted below.

[00019] Definitions to be used within this process and method include security, secure environment, environment Risk Factor, and individual Risk Factor.

[00020] Security refers to methods to control access to a secure environment.

[00021] A secure environment can be an airport, a train station, a computer program, a facility such as a building like an office or a warehouse or a parking garage, a country border, a common carrier, like an airplane, a train, a laboratory, a school, a military base, a private company complex, a monument or government building, or similar structures.

[00022] Other examples of secured environments include the Pentagon, airports, train stations, bus terminals, sports facilities like stadiums, casinos, hotels, large venue entertainment areas, like the MGM Grand convention complex, large venue trade shows, like the Sands Convention Center in Las Vegas.

[00023] The environment Risk Factor is an arbitrary designation associated with a secured environment or location. The environment Risk Factor is assigned by the owner of the secured environment based upon the level of access the owner wishes to maintain in the area. If the secured area is a special laboratory where a company to doing research and development, the owner may want to assign a high environment Risk Factor in order to limit the access to the area only to people with a high clearance code.

[00024] The individual Risk Factor is an arbitrary designation associated with a given individual. The individual Risk Factor is compared against the environment Risk Factor in order to determine whether the individual can enter a given location.

[00025] The methods contemplate that the individual Risk Factors can be letter designations, number designations, alpha-numeric designations, or similar types assigned values. The individual Risk Factors need to be of the sort that are comparable so a determination can be made as to whether an individual is an authorized individual.

[00026] For illustrative purposes, the individual Risk Factors could include four classes: Risk Factor 0, Risk Factor I, Risk Factor II, or Risk Factor III.

[00027] A Risk Factor 0 can mean that no designated risk factors assigned to an individual at this time and that the individual is "OK" to proceed into the secure environment. Risk Factor 0 individuals are those who have been assessed for risk, their individual information has been entered into the system and is complete, and it is safe for them to proceed into the secure environment. For individuals who have not yet been assessed for risk they are automatically assigned Risk Factor I, with involves using a set of criteria on the individual in order to enter them into the system.

[00028] If the owner did not assign a Risk Factor 0 to the individual, a Risk Factor I could be assigned. The owner would obtain information pertaining to the individual Examples of this type of information can include the individual's name, individual's address, nationality, height, approximate weight, social security number or passport number or government identification type and number, credit card number, a finger print, a digital photo, or age of individual.

[00029] If the owner believes the individual carries a risk to the secured area beyond a Risk Factor 0 or I assessment, the owner can assign a Risk Factor II. Risk Factor II assessments would result from the cross comparison of the data entered on the individual to other information and other databases, such as Interpol databases, immigration database, FBI and CIA databases and similar police linked databases. The information from other databases could include information pertaining to

a. former prison inmate and parole status;

b. times and dates of prior admissions and prior denials to this secure environment or similarly rated secure environments;

c. prior seizures of items prohibited in the secure environment, such as knives, guns, weapons, chemical explosives;

d. "wanted" list information; and

e. pending court judgments.

[00030] If any of the above indicators are not clear, the individual is then given a Risk Factor III. When the owner obtains this information, the owner may make the determination that the individual poses a threat to the secured environment and, therefore, assign a Risk Factor II to the individual.

[00031] The owner may also inquire about other information pertaining to the individual. The information may be gathered from the authentication database, secondary databases, or by questioning. Topics for questions individuals with a Risk Factor include:

a. questions about the individual's most recent travels;

b. questions pertaining to immigration;

c. questions about the individual's police record and recent arrest;

d. questions about the individual's occupation; and

e. questions about the individual's possessions.

[00032] In this example, Risk Factor III means that the owner believes the individual is the highest risk to the secure environment. The owner may require the individual to be held for a search and further questions from government authorities, such as the police or the FBI.

[00033] If an individual an acceptable Risk Factor for the secured location and is permitted entry to the secure environment, a smart card or biometric device can be issued to the individual that permits access using the smart card or biometric device for that certain secure environment.

[00034] The biometric card is not contemplated for use when the individual is cleared for one secure environment, but not all secured locations. Even with the smart card or biometric device, it is still contemplated that an individual is assigned a risk level for a point of entry so that even if an individual gains entry at one point of entry, they do

not gain entry to a second point of entry that may have a higher standard and requires a different evaluation.

[00035] Referring to FIG 1, an embodiment is a method for providing access and tracking the access of a non-registered individual at a secure point of entry to a secure environment.

[00036] The initial step of the method involves the owner establishing the secure environment (105). The secured environment needs a secure point of entry and an environment Risk Factor assigned to the environment. The owner assigns the secured environment an environment Risk Factor based upon the level of security the owner wants for the area.

[00037] Next, an individual with an identification information requests entry into the secured environment at the secure point of entry (110). The identification information includes an individual identifier. The identification information can be one or a collection of unique designations that separates one individual from another, such a name, an alpha-numeric code, a fingerprint, or any other biometric characteristic. The individual identifier is the unique designation that is sent to the authentication database in order to verify the identity of the individual.

[00038] The individual can request entry into the secured environment by using an interface, such as a fingerprint reader, a numerical code, a voice pattern recognition reader, a retinal scanner, a telemetry card reader, a smart card reader, other biometric readers, or combinations thereof. The individual can also request entry into the secured environment by using a secondary party, such as a secretary, a clerk, an employee, a security guard, a contract worker, or combinations thereof.

[00039] Continuing with FIG 1, the method then entails sending the individual identifier to an authentication database (115). The authentication database is a collection of records for registered individuals stating, at the least, the individual identifier and the assigned Risk Factor. The method contemplates that the authentication database is

established by a third party who is neither the individual nor the owner of the secured environment.

[00040] The individual identifier can also be cross-referenced as a background check of the individual with other information obtained from various other stored databases via Internet links. The authentication database can be linked to secondary databases, such as Interpol database, United States Border Patrol database; US police database, US FBI database, US CIA database, state agency fingerprint databases, and other state authentication database, immigration databases, or combinations thereof.

[00041] The authentication database searches the database for the individual identifier. When the individual identifier is not found, the authentication database sends a response to the owner stating that the individual is a non-registered individual (120).

[00042] Continuing with FIG 1, the method then involves the owner asking the non-registered individual a plurality of questions (125). The individual's answers to the questions produce a profile. The owner then assigns the individual a Risk Factor based upon the profile (130).

[00043] If the owner believes that individual poses a great risk, the method contemplates that the individual can be held until additional authorities are notified. Examples of authorites include police, FBI, CIA, Border Patrol, Immigration, Interpol and other police.

[00044] The method continues by the owner registering the non-registered individual with the individual Risk Factor on the authentication database (135). Since the individual was not present in the authentication database, this step of the method entails the owner creating a record in the authentication database. At a minimum the record has the individual identifier and the individual Risk Factor. The record can include other information relevant to the individual.

[00045] As seen in FIG 1, the method ends by making a comparison between the individual Risk Factor and the environment Risk Factor (140); making a determination whether the individual is allowed entry into the secured environment based upon the

comparison (145); and adding the determination to the record of the individual in the authentication database (150).

[00046] In an alternative embodiment of the method, the individual information and identifier is stored on a smart card for entry into the database and the smart card is only usable by the individual with the proper biometric key.

[00047] Referring to FIG 2, an embodiment is a method providing access and tracking of the access of a registered individual at a secure point of entry to a secure environment.

[00048] The initial steps of method mirror the embodiment of the method for a non-registered individual. The method entails an owner establishing the secure environment with a secure point of entry and an assigned environment Risk Factor (205) and an individual with an individual identifier requesting entry into the secured environment at the secure point of entry (210).

[00049] The individual identifier is sent to the authentication database (215). The individual identifier is checked against the records in the authentication database.

[00050] A response is sent to the owner stating that the individual is registered (220). The response also includes the individual Risk Factor assigned to the individual by the owner.

[00051] As seen in FIG 2, the method continues by making a comparison between the individual Risk Factor and the environment Risk Factor (225) and making a determination whether the individual is allowed entry into the secured environment based upon the comparison (230).

[00052] In an alternative embodiment, the owner may decide to ask the individual a series of questions in order to create a profile. The owner than may decide to modify the individual Risk Factor assigned to the individual based upon the profile. In addition, the owner can decide that the individual now poses a risk to the secured environment and can hold the individual until additional authorities are notified.

[00053] The method ends by adding the determination to the record of the individual in the

authentication database (235).

[00054] The individual information in the method is stored on a smart card for entry into the authentication database. The smart card is only usable by the individual with the proper biometric key.

[00055] The method and process contemplate the authentication database can also include a template for issuing notifications or alarms when an individual does not comply with a Risk Factor assigned to gain entry to a certain secure environment. This template would include:

a. criteria input by an owner or government authority that an individual must meet in order to gain entry to a secure environment, such as

   i. questions asking who an individual represents;

   ii. questions asking what is the purpose of an individual's activity at the secure environment;

   iii. questions asking for individual information; and

   iv. names of individuals who are granted a Risk Factor 0 and permitted entry;

b. individual information.

[00056] The predetermined template used in the method includes criteria used by the owner of the secure environment. The predetermined template can also include a statement or information from a governmental or other authority where the individual is disallowed entry to the secure environment pending a search or questioning. It is contemplated to be within the scope of the method that an owner has a list of persons who are permitted to enter the secure environment.

[00057] While this method has been described with emphasis on the preferred embodiments, it should be understood that within the scope of the appended claims the method might be practiced other than as specifically described herein.